Configuring a Dynamic Shared Secret for the Cisco CMTS

This document describes the Dynamic Shared Secret feature, which enables service providers to provide higher levels of security for their Data-over-Cable Service Interface Specifications (DOCSIS) cable networks. This feature uses randomized, single-use shared secrets to verify the DOCSIS configuration files that are downloaded to each cable modem.

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent-pending feature is designed to guarantee that all registered modems are using only the quality of service (QoS) parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

Feature Specifications for Dynamic Shared Secret

Feature History	
Release	**Modification**
Release 12.2(15)BC1	This feature was introduced.
Release 12.2(15)BC1b	Support for the **nocrypt** option was added to the **cable dynamic-secret** command.
Release 12.2(15)BC2	SNMP support for the Dynamic Shared Secret feature was added to CISCO-DOCS-EXT-MIB, and a new option (**dmic-lock**) was added to the **snmp-server enable traps cable** command.
Release 12.3(9a)BC	The **cable dynamic-secret exclude** command was added to allow specific cable modems to be excluded from the Dynamic Shared Secret feature.
Release 12.3(17a)BC	The DMIC lock mode behavior is revised to support additional security during N+1 Redundancy switchover events. Refer to the "Restrictions for Dynamic Shared Secret" section on page 3 for additional information.
Supported Platforms	
Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 routers	

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

This document includes the following major sections:

Prerequisites for Dynamic Shared Secret

The Dynamic Shared Secret feature has the following prerequisites:

- The Cisco CMTS must be running Cisco IOS Release 12.2(15)BC1 or later Cisco IOS Release 12.2 BC or 12.3 BC release.
- The Dynamic Shared Secret feature supports either an external provisioning server or the CMTS acting as the TFTP server (using either DOCSIS configuration files stored in Flash memory or using the internal DOCSIS configuration file editor). If you are using the CMTS as the TFTP server, you must also meet the prerequisites given in the "Additional References" section on page 27.
- A cable modem must be able to register with the Cisco CMTS before enabling the Dynamic Shared Secret feature.
- It is optional, but highly recommended, that you also configure a shared secret on each cable interface, and use that shared secret to create the DOCSIS configuration files for those cable modems. You can also optionally configure up to 16 secondary shared secrets on each cable interface. This is not required to use the Dynamic Shared Secret feature, but it does provide another layer of security, because the CMTS uses the manually configured shared secret to verify the original DOCSIS configuration files that it downloads from the TFTP server.

Note If a manually configured shared secret is configured, it *must* match the shared secret that was used to create the DOCSIS configuration files. If the configuration file cannot be verified against the shared secret (and any secondary shared secrets that might be configured), the CMTS does not allow any cable modems using that configuration file to come online, regardless of the Dynamic Shared Secret configuration.

- It is optional to also configure the **cable tftp-enforce** command on each cable interface to require that cable modems download their DOCSIS configuration files through the CMTS. This identifies, on a per-modem basis, those users who are attempting to bypass the shared secret checks by downloading a DOCSIS configuration file from a local TFTP server.

  When the **cable tftp-enforce** command is used with the **cable dynamic-secret** command, the TFTP enforce checks are done before the dynamic shared-secret checks. If a cable modem fails to download a DOCSIS configuration file through the CMTS, it is not allowed to register, regardless of the dynamic shared-secret checks.
- The Dynamic Shared Secret feature is compatible with cable modems that are DOCSIS 1.0-, DOCSIS 1.1-, and DOCSIS 2.0-certified, which are operating in any valid DOCSIS mode.
- For full security, DOCSIS configuration files should have filenames that are at least 5 or more characters in length.
- For best performance during the provisioning of cable modems, we recommend using Cisco Network Registrar Release 3.5 or later. (See the "Performance Information" section on page 10.)

Note When the Dynamic Shared Secret feature is enabled using its default configuration, a cable modem diagnostic webpage shows a scrambled name for its DOCSIS configuration file. This filename changes randomly each time that the cable modem registers with the CMTS. To change the default behavior, use the **nocrypt** option with the **cable dynamic-secret** command.

Restrictions for Dynamic Shared Secret

General Restrictions for Dynamic Shared Secret

- If you configure the Dynamic Shared Secret feature on a master cable interface, you should also configure the feature on all of the corresponding slave cable interfaces.
- The Dynamic Shared Secret feature ensures that each cable modem registering with the CMTS can use only the DOCSIS configuration file that is specified by the service provider's authorized Dynamic Host Configuration Protocol (DHCP) and TFTP servers, using the DOCSIS-specified procedures.
- The Dynamic Shared Secret feature does not affect cable modems that are already online and provisioned. If a cable modem is online, you must reset it, so that it reregisters, before it complies with the Dynamic Shared Secret feature.
- The DMIC lock mode uses the following behavior during a switchover event in HCCP N+1 Redundancy, commencing in Cisco IOS Release 12.3(17a)BC. All cable modems which were previously in lock mode are taken offline during a switchover event, and the prior state of locked modems is lost. If previously locked modems remain non-compliant, they will return to LOCK mode after three failed registration attempts. If the modems have become DOCSIS compliant, they will return online in the normal fashion. Refer to the "SNMP Support" section on page 10 for additional information about DMIC lock mode.
- The Cisco uBR7100 series router does not support the Dynamic Shared Secret feature when running in MxU bridging mode.
- If a Broadband Access Center for Cable (BACC) provisioning server is being used, the Device Provisioning Engine (DPE) TFTP server verifies that the IP address of the TFTP client matches the expected DOCSIS cable modem IP Address. If a match is not found, the request is dropped. This

functionality is incompatible with the CMTS DMIC feature. Use the **no tftp verify-ip** command on all BACC DPE servers to disable the verification of the requestor IP address on dynamic configuration TFTP requests. Refer to the Cisco Broadband Access Centre DEP CLI Reference, 2.7.1 in the "Related Documents" section on page 27 for additional information.

Cable Modem Restrictions for Dynamic Shared Secret

DHCP Restriction for Incognito Server and Thomson Cable Modems

The Dynamic Host Configuration Protocol (DHCP) passes configuration information to DHCP hosts on a TCP/IP network. Configuration parameters and other control information are stored in the `options` field of the DHCP message.

When using DMIC with the Incognito DHCP server, the Incognito server must be re-configured so that the following two options are *not* sent in the DHCP message:

- *option 66*—This option is used to identify a TFTP server when the `sname` field in the DHCP header has been used for DHCP options. Option 66 is a variable-length field in the Options field of a DHCP message described as "an option used to identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options," as per RFC 2132.
- *sname field*—The sname field is a 64-octet field in the header of a DHCP message described as "optional server host name, null terminated string," as per RFC2131. A DHCP server inserts this option if the returned parameters exceed the usual space allotted for options. If this option is present, the client interprets the specified additional fields after it concludes interpretation of the standard option fields.

Note It is not compliant with DOCSIS to include both of these options in the DHCP message.

The problematic packet capture below is a DHCP offer in which both sname and option 66 are set (in this respective sequence):

```
0000  00 30 19 47 8f 00 00 d0 b7 aa 95 50 08 00 45 00
0010  01 4a 8f 50 00 00 80 11 46 30 ac 10 02 01 ac 10
0020  0a 01 00 43 00 43 01 36 0c 75 02 01 06 00 b0 a0
0030  25 01 00 00 00 00 00 00 00 00 ac 10 0a 53 00 00
0040  00 00 ac 10 0a 01 00 10 95 25 a0 b0 00 00 00 00
0050  00 00 00 00 00 00 5b 31 37 32 2e 31 36 2e 32 2e
(sname option immediately above)
0060  31 5d 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 64 65 66 61 75 6c 74 2e 63 66
00a0  67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110  00 00 00 00 00 00 63 82 53 63 35 01 02 36 04 ac
0120  10 02 01 33 04 00 06 94 0d 01 04 ff ff ff 00 02
0130  04 ff ff b9 b0 03 08 ac 10 02 fe ac 10 0a 01 04
0140  04 ac 10 02 01 07 04 ac 10 02 01 42 0a 31 37 32
(option 66 immediately above)
0150  2e 31 36 2e 32 2e 31 ff
```

When using DMIC with Incognito DHCP servers and Thomson cable modems, you must prevent both options from being sent in the DHCP offer. Use one of the following workaround methods to achieve this:

- Change the Incognito DHCP server so that it does not include the sname option as described above.
- Change the cable modem code so that sname is not prioritized above option 66, as in the problematic packet capture shown in the example above.
- Upgrade your installation of Cisco IOS to Release 12.3(9a)BC4 or a later release. These releases can exclude Thomson cable modems from the Cable dynamic secret feature by excluding the OUI setting.

  Note The above method is not secure.

- Migrate to a compliant DHCP and TFTP server such as CNR. This also offers significantly higher performance.

Refer to these resources for additional DOCSIS DHCP information, or optional DHCP MAC exclusion:

- *DHCP Options and BOOTP Vendor Extensions, RFC 2132*

  http://www.ietf.org/rfc/rfc2132.txt
- *Filtering Cable DHCP Lease Queries on Cisco CMTS Routers*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.html

DOCSIS Compliance

- Cable modems are assumed to be DOCSIS-compliant. If a cable modem is not fully DOCSIS-compliant, it could trigger a CMTS Message Integrity Check (MIC) failure during registration in rare circumstances. Under normal operations, however, it can be assumed that cable modems that fail the CMTS MIC check from the Dynamic Shared Secret feature are either not DOCSIS-compliant, or they might have been hacked by the end user to circumvent DOCSIS security features.

  Some of the cable modems with the following OUIs have been identified as having problems with the Dynamic Shared Secret feature, depending on the hardware and software revisions:

  - 00.01.03
  - 00.E0.6F
  - 00.02.B2

  These particular cable modems can remain stuck in the init(o) MAC state and cannot come online until the Dynamic Shared Secret feature is disabled. If this problem occurs, Cisco recommends upgrading the cable modem's software to a fully compliant software revision.

  Alternatively, these cable modems may be excluded from the *dynamic* secret function using the following command in global configuration mode:

  cable dynamic-secret exclude {**oui** *oui-id* | **modem** *mac-address*}

  Excluding cable modems means that if a violator chooses to modify their cable modem to use one of the excluded OUIs, then the system is no longer protected. Refer to the "Excluding Cable Modems from the Dynamic Shared Secret Feature" section on page 18.

Tip To help providers to identify non-DOCSIS compliant modems in their network, the Dynamic Shared Secret feature supports a “mark-only” option. When operating in the mark-only mode, cable modems might be able to successfully obtain higher classes of service than are provisioned, but these cable modems will be marked as miscreant in the **show cable modem** displays (with **!online**, for example). Such cable modems also display with the **show cable modem rogue** command.

Service providers may decide whether those cable modems must be upgraded to DOCSIS-compliant software, or whether the end users have hacked the cable modems for a theft-of-service attack.

The following example illustrates output from a Cisco CMTS that is configured with the **cable dynamic-secret mark** command with miscreant cable modems installed. These cable modems may briefly show up as "reject(m)" for up to three registration cycles before achieving the **!online** status.

```
Router# show cable modem rogue
                                        Spoof TFTP
MAC Address    Vendor     Interface     Count Dnld Dynamic Secret
000f.0000.0133 00.0F.00   C4/0/U1       3     Yes  905B740F906B48870B3A9C5E441CDC67
000f.0000.0130 00.0F.00   C4/0/U1       3     Yes  051AEA93062A984F55B7AAC979D10901
000f.0000.0132 00.0F.00   C4/0/U2       3     Yes  FEDC1A6DA5C92B17B23AFD2BBFBAD9E1

vxr#scm | inc 000f
000f.0000.0133 4.174.4.101     C4/0/U1  !online       1     -7.00 2816    0   N
000f.0000.0130 4.174.4.89      C4/0/U1  !online       2     -6.50 2819    0   N
000f.0000.0132 4.174.4.90      C4/0/U2  !online       18    -7.00 2819    0   N
```

TFTP Restrictions

- Cable modems can become stuck in the TFTP transfer state (this is indicated as init(o) by the **show cable modem** command) in the following situations:
  - The Dynamic Shared Secret feature is enabled on the cable interface, using the **cable dynamic-secret** command. This feature applies if the cable modem is a miscreant cable modem, or if the cable modem is a DOCSIS 1.0 cable modem running early DOCSIS 1.0 firmware that has not yet been updated. This feature also applies if the TFTP server is unable to provide the cable modem's TFTP configuration file to the Cisco CMTS. This is the case, for example, when using BACC and not configuring the system to permit a TFTP request from a non-matching source IP address. The **debug cable dynamic-secret** command also shows this failure.
  - The cable modems on that interface are downloading a DOCSIS configuration file that is greater than 4 Kbytes in size. This condition applies when using a Cisco IOS release prior to 12.3(15)BC4.
  - A large number of cable modems are registering at the same time. Some or all of those cable modems could also be downloading the DOCSIS configuration file using multiple TFTP transfers that use multiple TFTP ports on the Cisco CMTS router, and the TFTP server is unable to keep up with the rate of TFTP requests generated by the system. Some TFTP servers may be limited to the number of concurrent TFTP get requests initiated by the same source IP address per unit time, or simply unable to handle the rate of new modem registrations before cable dynamic-secret is configured. The **debug cable dynamic-secret** command shows failure to receive some files in this situation.
  - There is a mismatch in the shared secret between the Cisco CMTS and the DOCSIS configuration file. In this situation, the cable modems are stuck in init(o) state, when the cable shared feature and DMIC are enabled on the Cisco CMTS router.

This situation of stuck cable modems can result in the TFTP server running out of available ports, resulting in the cable modems failing the TFTP download stage. To prevent this situation from happening, temporarily disable the Dynamic Shared Secret feature on the cable interface or reduce the size of the DOCSIS configuration file.

Individual cable modems may react better if they are power cycled after DMIC is enabled or disabled as they have trouble changing the TFTP server IP address for the DOCSIS config file. While this behavior has been indicated for older modems, it has not yet been reproduced consistently in the lab at large scale.

Information About Dynamic Shared Secret

This section describes the Dynamic Shared Secret feature:

Feature Overview

The DOCSIS specifications require that cable modems download, from an authorized TFTP server, a DOCSIS configuration file that specifies the quality of service (QoS) and other parameters for the network session. Theft-of-service attempts frequently attempt to intercept, modify, or substitute the authorized DOCSIS configuration file, or to download the file from a local TFTP server.

To prevent theft-of-service attempts, the DOCSIS specification allows service providers to use a shared secret password to calculate the CMTS Message Integrity Check (MIC) field that is attached to all DOCSIS configuration files. The CMTS MIC is an MD5 digest that is calculated over the DOCSIS Type/Length/Value (TLV) fields that are specified in the configuration file, and if a shared secret is being used, it is used in the MD5 calculation as well.

The cable modem must include its calculation of the CMTS MIC in its registration request, along with the contents of the DOCSIS configuration file. If a user modifies any of the fields in the DOCSIS configuration file, or uses a different shared secret value, the CMTS cannot verify the CMTS MIC when the cable modem registers. The CMTS does not allow the cable modem to register, and marks it as being in the “reject(m)” state to indicate a CMTS MIC failure.

Users, however, have used various techniques to circumvent these security checks, so that they can obtain configuration files that provide premium services, and then to use those files to provide themselves with higher classes of services. Service providers have responded by changing the shared secret, implementing DOCSIS time stamps, and using modem-specific configuration files, but this has meant creating DOCSIS configuration files for every cable modem on the network. Plus, these responses would have to be repeated whenever a shared secret has been discovered.

The Dynamic Shared Secret feature prevents these types of attacks by implementing a dynamically generated shared secret that is unique for each cable modem on the network. In addition, the dynamic shared secrets are valid only for the current session and cannot be reused, which removes the threat of “replay attacks,” as well as the reuse of modified and substituted DOCSIS configuration files.

Modes of Operation

The Dynamic Shared Secret feature can operate in three different modes, depending on what action should be taken for cable modems that fail the CMTS MIC verification check:

- Marking Mode—When using the **mark** option, the CMTS allows cable modems to come online even if they fail the CMTS MIC validity check. However, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.
- Locking Mode—When the **lock** option is used, the CMTS assigns a restrictive QoS configuration to CMs that fail the MIC validity check twice in a row. You can specify a particular QoS profile to be used for locked cable modems, or the CMTS defaults to special QoS profile that limits the downstream and upstream service flows to a maximum rate of 10 kbps.

  If a customer resets their CM, the CM will reregister but still uses the restricted QoS profile. A locked CM continues with the restricted QoS profile until it goes offline and remains offline for at least 24 hours, at which point it is allowed to reregister with a valid DOCSIS configuration file. A system operator can manually clear the lock on a CM by using the **clear cable modem lock** command.

  This option frustrates users who are repeatedly registering with the CMTS in an attempt to guess the shared secret, or to determine the details of the Dynamic Shared Secret security system.
- Reject Mode—In the reject mode, the CMTS refuses to allow CMs to come online if they fail the CMTS MIC validity check. These cable modems are identified in the **show cable modem** displays with a MAC state of "reject(m)" (bad MIC value). After a short timeout period, the CM attempts to reregister with the CMTS. The CM must register with a valid DOCSIS configuration file before being allowed to come online. When it does come online, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.

Note To account for possible network problems, such as loss of packets and congestion, the Cisco CMTS will allow a cable modem to attempt to register twice before marking it as having failed the Dynamic Shared Secret authentication checks.

Operation of the Dynamic Shared Secret

The Dynamic Shared Secret feature automatically creates a unique DOCSIS shared secret on a per-modem basis, creating a one-time use DOCSIS configuration file that is valid only for the current session. This ensures that a DOCSIS configuration file that has been downloaded for one cable modem can never be used by any other modem, nor can the same modem reuse this configuration file at a later time.

This patent pending feature is designed to guarantee that all registered modems are using only the QOS parameters that have been specified by the DOCSIS provisioning system for that particular modem at the time of its registration.

When a DOCSIS-compliant cable modem registers with the CMTS, it sends a DHCP request, and the DHCP server sends a DHCP response that contains the name of the DOCSIS configuration file that the cable modem should download from the specified TFTP server. The cable modem downloads the DOCSIS configuration file and uses its parameters to register with the CMTS.

When the Dynamic Shared Secret feature is enabled, the CMTS performs the following when it receives the DHCP messages:

- The CMTS creates a dynamically generated shared secret.

- In the default configuration, the CMTS takes the name of the DOCSIS configuration file and generates a new, randomized filename. This randomized filename changes every time the cable modem registers, which prevents the caching of DOCSIS configuration files by cable modems that are only semi-compliant with the DOCSIS specifications. You can disable this randomization of the filename by using the **nocrypt** option with the **cable dynamic-secret** command.
- The CMTS changes the IP address of the TFTP server that the cable modem should use to the IP address of the CMTS. This informs the cable modem that it should download its configuration file from the CMTS.
- The CMTS downloads the original DOCSIS configuration file from the originally specified TFTP server so that it can modify the file to use the newly generated dynamic secret.

When the cable modem downloads the DOCSIS configuration file, it receives the modified file from the CMTS. Because this file uses the one-time-use dynamically generated shared secret, the CMTS can verify that the cable modem is using this configuration file when it attempts to register with the CMTS.

Note The Dynamic Shared Secret feature does not affect the use of the original shared secret or secondary shared secrets that are configured using the **cable shared-secondary-secret** and **cable shared-secret** commands. If these shared secrets are configured, the Cisco CMTS continues to use them to validate the original DOCSIS configuration file that is downloaded from the TFTP server. If the DOCSIS configuration file fails to pass the original or secondary shared secret verification checks, the cable modem is not allowed to register, and the Dynamic Shared Secret feature is not invoked for that particular cable modem.

Tip Although a user could attempt to circumvent these checks by downloading a DOCSIS configuration file from a local TFTP server, the cable modem would still fail the CMTS MIC verification. To identify users who are attempting to use a locally downloaded configuration file, use the **cable tftp-enforce** command.

Interaction with Different Commands

The Dynamic Shared Secret feature works together with a number of other commands to ensure network security and integrity:

- **cable config-file**—This command enables the Cisco CMTS internal DOCSIS configuration file editor, which creates DOCSIS configuration files as part of the router's configuration. The Cisco CMTS can transmit these files to cable modems using its onboard TFTP server. The Dynamic Shared Secret feature can be used together with these DOCSIS configuration files.
- **cable qos permission**—The **enforce** option with this command allows you to require a cable modem to use a specific, CMTS-provided QoS profile. This command can be used with the Dynamic Shared Secret feature, but if the dynamic shared-secret lock option is used, the QoS profile specified by the **cable qos permission enforce** command takes precedence over that specified using the **lock** option.
- **cable shared-secret**—The DOCSIS specification allows service providers to use a shared-secret to ensure that cable modems are using only authorized DOCSIS configuration files. The Dynamic Shared Secret feature enhances this security by providing another layer of security. Cable modems must successfully pass all shared-secret checks to come online.
- **cable shared-secondary-secret**—For flexible network management, the Cisco CMTS allows you to configure additional shared secrets on a cable interface. If a cable modem fails the primary shared-secret checks, the CMTS checks the modem against the secondary shared-secrets. This allows cable providers to regularly change their shared secrets without having to update all cable

modems at once. The Dynamic Shared Secret feature works together with this feature, so that if primary and secondary shared-secrets are configured, cable modems must pass at least one of those checks, as well as the dynamic shared-secret checks, before being allowed to come online.

- **cable tftp-enforce**—This command requires that cable modems download a DOCSIS configuration file over the cable interface before being allowed to come online. If a cable modem fails the TFTP-enforce checks, it is not allowed to come online. This command, along with the Dynamic Shared Secret feature, prevents the most comment theft-of-service attacks in which users try to substitute their own configuration files or try to modify the service provider's files.
- **tftp-server**—This command enables the TFTP server that is onboard the Cisco CMTS router, allowing it to deliver DOCSIS configuration files to cable modems. The DOCSIS configuration files can already be saved in the router's Flash memory, or you can create them using the router's internal DOCSIS configuration file editor. The Dynamic Shared Secret feature can be used with both types of DOCSIS configuration files and the onboard TFTP server.

Performance Information

The Dynamic Shared Secret feature does not add any additional steps to the cable modem registration process, nor does it add any additional requirements to the current provisioning systems. This feature can have either a small negative or a small positive effect on the performance of the network provisioning system, depending on the following factors:

- The provisioning system (DHCP and TFTP servers) being used
- The number of cable modems that are coming online
- The vendor and software versions of the cable modems
- The number and size of the DOCSIS configuration files

Large-scale testing has shown that the Dynamic Shared Secret feature can affect the time it takes for cable modems to come online from 5% slower to 10% faster. The most significant factor in the performance of the provisioning process is the provisioning system itself. For this reason, Cisco recommends using Cisco Network Registrar (CNR) Release 3.5 or greater, which can provide significant performance improvements over generic DHCP and TFTP servers.

The second-most important factor in the performance of cable modem provisioning is the number and size of the DOCSIS configuration files. The size of the configuration file determines how long it takes to transmit the file to the cable modem, while the number of configuration files can impact how efficiently the system keeps the files in its internal cache, allowing it to reuse identical configuration files for multiple modems.

SNMP Support

Cisco IOS Release 12.2(15)BC2 and later releases add the following SNMP support for the Dynamic Shared Secret feature:

- Adds the following MIB objects to the CISCO-DOCS-EXT-MIB:
  - cdxCmtsCmDMICMode—Sets and shows the configuration of the Dynamic Shared Secret feature for a specific cable modem (not configured, mark, lock, or reject).
  - cdxCmtsCmDMICLockQoS—Specifies the restrictive QoS profile assigned to a cable modem that has failed the Dynamic Shared Secret security checks, when the interface has been configured for lock mode.

  - cdxCmtsCmStatusDMICTable—Lists all cable modems that have failed the Dynamic Shared Secret security checks.

- An SNMP trap (cdxCmtsCmDMICLockNotification) can be sent when a cable modem is locked for failing the Dynamic Shared Secret security checks. The trap can be enabled using the **snmp-server enable traps cable dmic-lock** command.

Note The DMIC lock mode is disabled during a switchover event in HCCP N+1 Redundancy.

System Error Messages

Cisco IOS Release 12.2(15)BC1 and later releases display the following system error messages to provide information about cable modems that have failed the CMTS Message Integrity Check (MIC) when the Dynamic Shared Secret feature is enabled.

```
%UBR7100-4-BADCFGFILE
%UBR7200-4-BADCFGFILE
%UBR10000-4-BADCFGFILE: Modem config file [chars] at [integer]: [chars]
```

Explanation The DOCSIS configuration file for the cable modem failed its CMTS MIC verification, either because the MIC is missing or because the CMTS MIC failed verification with the shared secret or secondary shared secrets that have been configured for the cable interface. This message occurs when the dynamic secret feature is enabled on the cable interface with the **cable dynamic-secret** command.

Recommended Action Verify that the DOCSIS configuration file for the cable modem has been created using the correct shared secret value. Also verify that the DHCP server is specifying the proper configuration file for this cable modem, and that the configuration file on the TFTP server is the correct one.

Use the **show cable modem** command to display the MAC state for this particular cable modem. If the cable modem will remain in the "init(t)" state continually when the Dynamic Shared Secret feature is enabled, check for the following possible problems:

- The shared secret and secondary shared secrets that are configured on the cable interface do not match the ones that were used to create the DOCSIS configuration files. Either reconfigure the cable interface with the correct shared secret, or recreate the DOCSIS configuration files using the correct shared secret.
- The provisioning server is specifying the wrong DOCSIS configuration file for this cable modem.
- The DOCSIS configuration file on the TFTP server is either corrupted or incorrectly named.
- A user has successfully substituted their own DOCSIS configuration file into the service provider's network.
- A cable modem has cached the DOCSIS configuration file, or a user is attempting to reuse a previously generated DOCSIS configuration file. This could also indicate a possible theft-of-service attempt by a user attempting to upload a modified DOCSIS configuration file into the operator's TFTP server.

```
%UBR7100-4-CMLOCKED
%UBR7200-4-CMLOCKED
%UBR10000-4-CMLOCKED: Cable Modem [enet] in [char] attempted theft of service
```

Explanation The cable modem's DOCSIS configuration file did not contain a Message Integrity Check (MIC) value that corresponds with the proper Dynamic Shared Secret that was used to encode it. The CMTS has, therefore, assigned a restrictive quality of service (QoS) configuration to this cable modem to limit its access to the network. The CMTS has also locked the cable modem so that it will remain locked in the restricted QoS configuration until it goes offline for at least 24 hours, at which point it is permitted to reregister and obtain normal service (assuming it is DOCSIS-compliant and using a valid DOCSIS configuration file).

Recommended Action This error message appears when the **cable dynamic-secret lock** command has been applied to a cable interface to enable the Dynamic Shared Secret feature for the DOCSIS configuration files on that cable interface. The cable modem has been allowed to register and come online, but with a QoS configuration that is limited to a maximum rate of 10 kbps for both the upstream and downstream flows. Check to ensure that this cable modem is not running old software that caches the previously used configuration file. Also check for a possible theft-of-service attempt by a user attempting to download a modified DOCSIS configuration file from a local TFTP server. The CM cannot reregister with a different QoS profile until it has been offline for 24 hours, without attempting to register, or you have manually cleared the lock using the **clear cable modem lock** command.

```
%UBR7100-4-CMMARKED
%UBR7200-4-CMMARKED
%UBR10000-4-CMMARKED: Cable Modem [enet] in [chars] attempted theft of service
```

Explanation The cable modem's DOCSIS configuration file did not contain a Message Integrity Check (MIC) value that corresponds with the proper dynamic shared secret that was used to encode it. The CMTS has allowed this modem to register and come online, but has marked it in the **show cable modem** displays with an exclamation point (!) so that the situation can be investigated.

Recommended Action This error message appears when the **cable dynamic-secret mark** command has been applied to a cable interface to enable the Dynamic Shared Secret feature for the DOCSIS configuration files on that cable interface. Check to ensure that this cable modem is not running old software that caches the previously used configuration file. Also check for a possible theft-of-service attempt by a user attempting to download a modified DOCSIS configuration file from a local TFTP server.

```
%UBR7100-4-NOCFGFILE
%UBR7200-4-NOCFGFILE
%UBR10000-4-NOCFGFILE: Cannot read modem config file [chars] from [integer]:
[chars]
```

Explanation The CMTS could not obtain the DOCSIS configuration file for this cable modem from the TFTP server. This message occurs when the Dynamic Shared Secret feature is enabled on the cable interface with the **cable dynamic-secret** command.

Recommended Action Verify that the CMTS has network connectivity with the TFTP server, and that the specified DOCSIS configuration file is available on the TFTP server. Check that the DHCP server is correctly configured to send the proper configuration filename in its DHCP response to the cable modem. Also verify that the DOCSIS configuration file is correctly formatted.

This problem could also occur if the TFTP server is offline or is overloaded to the point where it cannot respond promptly to new requests. It might also be seen if the interface between the CMTS and TFTP server is not correctly configured and flaps excessively.

Note This error indicates a problem with the provisioning system outside of the Cisco CMTS. Disabling the Dynamic Shared Secret feature does not clear the fault, nor does it allow cable modems to come online. You must first correct the problem with the provisioning system.

Benefits

The Dynamic Shared Secret feature provides the following benefits to cable service providers and their partners and customers:

Improves Network Security

Service providers do not need to worry about users discovering the shared secret value and using it to modify DOCSIS configuration files to give themselves higher levels of service. Even if a user were to discover the value of a dynamically generated shared secret, the user would not be able to use that shared secret again to register.

In addition, if a manually configured shared secret is also used, the CMTS uses it to verify the DOCSIS configuration files that it receives from the TFTP server, providing MD-5 authenticated transactions between the TFTP server and the CMTS. This prevents users from bypassing the Dynamic Shared Secret feature by attempting to spoof the IP address of the provider's TFTP server.

The generic TFTP server performance and error handling on the Cisco CMTS routers has been greatly improved to support the high performance that is required for rapidly provisioning cable modems.

Flexibility in Dealing with Possible Theft-of-Service Attempts

Service providers have the option of deciding what response to take when a DOCSIS configuration file fails its CMTS MIC check: mark that cable modem and allow the user online, reject the registration request and refuse to allow the user to come online until a valid DOCSIS configuration file is used, or lock the cable modem in a restricted QoS configuration until the modem remains offline for 24 hours. Locking malicious modems is the most effective deterrent against hackers, because it provides the maximum penalty and minimum reward for any user attempting a theft-of-service attack.

No Changes to Provisioning System Are Needed

Service providers can use the Dynamic Shared Secret feature without changing their provisioning or authentication systems. Existing DOCSIS configuration files can be used unchanged, and you do not need to change any existing shared secrets.

Tip If not already done, the service provider could also install access controls that allow only the CMTS routers to download DOCSIS configuration files from the TFTP servers.

No Changes to Cable Modems Are Needed

The Dynamic Shared Secret feature does not require any end-user changes or any changes to the cable modem configuration. This feature supports any DOCSIS 1.0, DOCSIS 1.1, or DOCSIS 2.0-compatible cable modem.

Note The Dynamic Shared Secret feature does not affect cable modems that are already online and provisioned. Cable modems that are already online when the feature is enabled or disabled remain online.

Simplifies Network Management

Service providers do not have to continually update the shared secrets on a cable interface whenever the files providing premium services become widely available. Instead, providers can use the same shared secret on a cable interface for significant periods of time, trusting in the Dynamic Shared Secret feature to provide unique, single-use shared secrets for each cable modem.

In addition, service providers do not have to manage unique DOCSIS configuration files for each cable modem. The same configuration file can be used for all users in the same service class, without affecting network security.

Related Features

The following features can be used with the Dynamic Shared Secret feature to enhance the overall security of the cable network. For information on these features, see the documents listed in the "Additional References" section on page 27.

- Baseline Privacy Interface Plus (BPI+) Authorization and Encryption—Provides a secure link between the cable modem and CMTS, preventing users from intercepting or modifying packets that are transmitted over the cable interface. BPI+ also provides for secure authorization of cable modems, using X.509 digital certificates, as well as a secure software download capability that ensures that software upgrades are not spoofed, intercepted, or altered.
- TFTP Server and Internal DOCSIS Configurator File Generator—The Cisco CMTS can act as a TFTP server, providing dynamically generated DOCSIS configuration files to cable modems. The Dynamic Shared Secret feature can be used with the DOCSIS configuration files created by the internal editor and delivered by the CMTS TFTP server.
- Shared Secrets—A shared secret can be manually configured on a cable interface using the **cable shared-secret** command. All cable modems on that interface must use DOCSIS configuration files with a CMTS MIC that has been calculated with that shared secret, before being allowed to come online. When used with the Dynamic Shared Secret feature, the CMTS uses the manually specified shared secret to verify the DOCSIS configuration files it downloads from the TFTP server, before it modifies them with the dynamically generated shared secret.

Tip When using both a manually configured shared secret and the Dynamic Shared Secret feature, when a modem's configuration file fails the manual shared secret verification, the modem remains in the "init(t)" state until it times out and reregisters. If a cable modem seems stuck in the "init(t)" state, it could be a failure of the manual shared secret verification.

- Secondary Shared Secrets—To allow service providers to change the shared secret on a cable interface, without also having to immediately change all the DOCSIS configuration files being used on that interface, a cable interface can be configured with up to 16 additional shared secrets, using the **cable shared-secondary-secret** command. When a service provider changes the primary shared secret on a cable interface, the service provider can configure the previous shared secret as a secondary secret. This allows cable modems to continue using the previous shared secret until the provider can update the configuration file with the new value.

- TFTP Enforce—To require cable modems to download a DOCSIS configuration file over the cable interface, through the CMTS, use the **cable tftp-enforce** command. This prevents a common theft-of-service attack, in which a user attempts to download a modified DOCSIS configuration file from a local TFTP server.

How to Configure the Dynamic Shared Secret Feature

The following sections describe how to enable and configure the Dynamic Shared Secret feature, to disable the feature, or to manually clear a lock on a cable modem.

- Enabling and Configuring the Dynamic Shared Secret Feature, page 15
- Disabling the Dynamic Shared Secret on a Cable Interface, page 17
- Excluding Cable Modems from the Dynamic Shared Secret Feature, page 18
- Clearing the Lock on One or More Cable Modems, page 19

Note All procedures begin and end at the privileged EXEC prompt (“Router#”).

Enabling and Configuring the Dynamic Shared Secret Feature

This section describes how to enable and configure the Dynamic Shared Secret feature on a cable interface.

SUMMARY STEPS

1. **configure terminal**
2. **cable qos permission create**
3. **cable qos permission update**
4. **snmp-server enable traps cable dmic-lock**
5. **interface cable** *interface*
6. **cable dynamic-secret** {**lock** [*lock-qos*] | **mark** | **reject**} [**nocrypt**]
7. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 2	**cable qos permission create**
	
	Example:
	`Router(config)# cable qos permission create`
	`Router(config)#`
		(Optional) If you are using the **lock** option in Step 6, and if you are not specifying a specific QoS profile to be used, you must allow cable modems to create their own QoS profiles.

Step 3	**cable qos permission update**
	
	Example:
	`Router(config)# cable qos permission update`
	`Router(config)#`
		(Optional) If you are using the **lock** option in Step 6, and if you are not specifying a specific QoS profile to be used, you must allow cable modems to update their own QoS profiles.

Step 4	**snmp-server enable traps cable dmic-lock**
	
	Example:
	`Router(config)# snmp-server enable traps cable dmic-lock`
	`Router(config)#`
		(Optional) Enables the sending of SNMP traps when a cable modem fails a dynamic shared-secret security check.

Step 5	**interface cable** *interface*
	
	Example:
	`Router(config)# interface cable 3/0`
	`Router(config-if)#`
		Enters interface configuration mode for the specified cable interface.

	Command or Action	Purpose

Step 6	**cable dynamic-secret** {**lock** [*lock-qos*] | **mark** | **reject**} [**nocrypt**]
	
	Example:
	`Router(config-if)# cable dynamic-secret lock`
	`or`
	`Router(config-if)# cable dynamic-secret lock 90`
	`or`
	`Router(config-if)# cable dynamic-secret mark`
	`or`
	`Router(config-if)# cable dynamic-secret reject`
	`Router(config-if)#`
		Enables the Dynamic Shared Secret feature on the cable interface and configures it for the appropriate option:
		• **nocrypt**—(Optional) The Cisco CMTS does not encrypt the filenames of DOCSIS configuration files, but sends the files to CMs using their original names.
		• **lock**—Cable modems that fail the MIC verification are allowed online with a restrictive QoS profile. The cable modems must remain offline for 24 hours to be able to reregister with a different QoS profile.
		• *lock-qos*—(Optional) Specifies the QoS profile that should be assigned to locked cable modems. The valid range is 1 to 256, and the profile must have already been created. If not specified, locked cable modems are assigned a QoS profile that limits service flows to 10 kbps (requires Step 2 and Step 3).
		• **mark**—Cable modems that fail the MIC verification are allowed online but are marked in the **show cable modem** displays so that the situation can be investigated.
		• **reject**—Cable modems that fail the MIC verification are not allowed to register.

	Note Repeat Step 5 and Step 6 for each cable interface to be configured.	

Step 7	**end**
	
	Example:
	`Router(config-if)# exit`
	`Router#`
		Exits interface configuration mode and returns to privileged EXEC mode.

Note If you configure the Dynamic Shared Secret feature on any interface in a cable interface bundle, you should configure it on all interfaces in that same bundle.

Disabling the Dynamic Shared Secret on a Cable Interface

This section describes how to disable the Dynamic Shared Secret feature on a cable interface. The cable modem continues to be validated against any shared secret or secondary shared secrets that have been defined on the cable interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface cable** *interface*
3. **no cable dynamic-secret**
4. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 2	**interface cable** *interface*
	
	Example:
	`Router(config)# interface cable 3/0`
	`Router(config-if)#`
		Enters interface configuration mode for the specified cable interface.

Step 3	**no cable dynamic-secret**
	
	Example:
	`Router(config-if)# no cable dynamic-secret`
	`Router(config-if)#`
		Disables the Dynamic Shared Secret feature on the cable interface.

	Note Repeat Step 2 and Step 3 for each cable interface to be configured.	

Step 4	**end**
	
	Example:
	`Router(config-if)# exit`
	`Router#`
		Exits interface configuration mode and returns to privileged EXEC mode.

Excluding Cable Modems from the Dynamic Shared Secret Feature

This section describes how to exclude one or more cable modems from being processed by the Dynamic Shared Secret feature. The cable modem continues to be validated against any shared secret or secondary shared secrets that have been defined on the cable interface.

SUMMARY STEPS

1. **configure terminal**
2. **cable dynamic-secret exclude** {**oui** *oui-id* | **modem** *mac-address*}
3. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 2	**cable dynamic-secret exclude** {**modem** *mac-address* | **oui** *oui-id*}
	
	Example:
	`Router(config)# cable dynamic-secret exclude oui 00.01.B4`
	`Router(config)# cable dynamic-secret exclude modem 00d0.45ba.b34b`
	`Router(config)#`
		Excludes one or more cable modems from being processed by the Dynamic Shared Secret security checks, on the basis of their MAC addresses or OUI values:
		• **modem** *mac-address*—Specifies the hardware (MAC) address of one specific and individual cable modem to be excluded from the Dynamic Shared Secret feature. (You cannot specify a multicast MAC address.)
		• **oui** *oui-id*—Specifies the organization unique identifier (OUI) of a vendor, so that a group of cable modems from this vendor are excluded from the Dynamic Shared Secret feature. The OUI should be specified as three hexadecimal bytes separated by either periods or colons.
		Note Repeat this command for each cable modem MAC address or OUI vendor to be excluded.

Step 3	**end**
	
	Example:
	`Router(config-if)# exit`
	`Router#`
		Exits interface configuration mode and returns to privileged EXEC mode.

Clearing the Lock on One or More Cable Modems

This section describes how to manually clear the lock on one or more cable modems. This forces the cable modems to reinitialize, and the cable modems must reregister with a valid DOCSIS configuration file before being allowed online. If you do not manually clear the lock (using the **clear cable modem lock** command), the cable modem is locked in its current restricted QoS profile and cannot reregister with a different profile until it has been offline for at least 24 hours.

SUMMARY STEPS

1. **clear cable modem** {*mac-addr* | *ip-addr* | **all** | **oui** *string* | **reject**} **lock**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**clear cable modem** {*mac-addr* | *ip-addr* | **all** | **oui** *string* | **reject**} **lock**
	
	Example:
	`Router# clear cable modem 0001.0203.0405 lock`
	`Router# clear cable modem all lock`
	`Router# clear cable modem oui 00.00.0C lock`
	`Router#`
		Clears the lock for the cable modems, which can be identified as follows:
		• *mac-addr*—Specifies the MAC address for one particular cable modem to be cleared.
		• *ip-addr*—Specifies the IP address for one particular cable modem to be cleared.
		• **all**—Clears the locks on all locked cable modems.
		• **oui** *string*—Clears the locks on all cable modems with a vendor ID that matches the specified Organizational Unique Identifier (OUI) string.
		• **reject**—Clears the locks on all cable modems that are currently in the reject state (which would occur if a locked cable modem went offline and attempted to reregister before 24 hours had elapsed).

Tip A cable modem can also be unlocked by manually deleting the cable modem from all CMTS internal databases, using the **clear cable modem delete** command.

Monitoring the Dynamic Shared Secret Feature

This section describes the following procedures you can use to monitor and display information about the Dynamic Shared Secret feature:

- Displaying Marked Cable Modems, page 20
- Displaying the Current Dynamic Secrets, page 21

Displaying Marked Cable Modems

When you configure a cable interface with the **cable dynamic-secret mark** command, cable modems that fail the dynamically generated CMTS MIC verification are allowed online, but are marked with an exclamation point (!) in the MAC state column in the **show cable modem** display. The exclamation point is also used to identify cable modems that were initially rejected, using the **cable dynamic-secret reject** command, but then reregistered using a valid DOCSIS configuration file.

For example, the following example shows that four cable modems are marked as having failed the CMTS MIC verification, but that they have been allowed online:

```
Router# show cable modems

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0010.9507.01db 144.205.151.130 C5/1/0/U5 online(pt)  1     0.25    938   1    N
0080.37b8.e99b 144.205.151.131 C5/1/0/U5 online      2    -0.25   1268   0    N
0002.fdfa.12ef 144.205.151.232 C6/1/0/U0 online(pt)  13   -0.25   1920   1    N
```

```
0002.fdfa.137d 144.205.151.160 C6/1/0/U0 !online     16    -0.50   1920  1    N
0003.e38f.e9ab 144.205.151.237 C6/1/0/U0 !online     3     -0.50   1926  1    N
0003.e3a6.8173 144.205.151.179 C6/1/1/U2 offline     4     0.50    1929  0    N
0003.e3a6.8195 144.205.151.219 C6/1/1/U2 !online(pt) 22    -0.50   1929  1    N
0006.28dc.37fd 144.205.151.244 C6/1/1/U2 online(pt)  61    0.00    1925  2    N
0006.28e9.81c9 144.205.151.138 C6/1/1/U2 online(pt)  2     0.75    1925  1    N
0006.28f9.8bbd 144.205.151.134 C6/1/1/U2 online      25    -0.25   1924  1    N
0006.28f9.9d19 144.205.151.144 C6/1/1/U2 online(pt)  28    0.25    1924  1    N
0010.7bed.9b6d 144.205.151.228 C6/1/1/U2 online(pt)  59    0.25    1554  1    N
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 online      15    -0.75   1914  1    N
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online      4     0.00    1917  1    N
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 !online     17    0.25    1919  1    N
0003.e38f.f4cb 144.205.151.238 C7/0/0/U5 online(pt)  16    0.00   !2750  1    N
0003.e3a6.7fd9 144.205.151.151 C7/0/0/U5 online      1     0.25    1922  0    N
0020.4005.3f06 144.205.151.145 C7/0/0/U0 online(pt)  2     0.00    1901  1    N
0020.4006.b010 144.205.151.164 C7/0/0/U5 online(pt)  3     0.00    1901  1    N
0050.7302.3d83 144.205.151.240 C7/0/0/U0 online(pt)  18    -0.25   1543  1    N
00b0.6478.ae8d 144.205.151.254 C7/0/0/U5 online(pt)  44    0.25    1920  21   N
00d0.bad3.c0cd 144.205.151.149 C7/0/0/U5 online      19    0.25    1543  1    N
00d0.bad3.c0cf 144.205.151.194 C7/0/0/U0 online      13    0.00    1546  1    N
00d0.bad3.c0d5 144.205.151.133 C7/0/0/U0 online      12    0.50    1546  1    N

Router#
```

You can also use the **show cable modem rogue** command to display only those cable modems that have been rejected for failing the dynamic shared-secret authentication checks:

```
Router# show cable modem rogue

                                    Spoof TFTP
MAC Address    Vendor     Interface  Count Dnld Dynamic Secret

AAAA.7b43.aa7f Vendor1    C4/0/U5        2  Yes  45494DC933F8F47A398F69EE6361B017
AAAA.7b43.aa7f Vendor1    C4/0/U5        2  Yes  D47BCBB5494E9936D51CB0EB66EF0B0A
BBBB.7b43.aa7f Vendor2    C4/0/U5        2  No   8EB196423170B26684BF6730C099D271
AAAA.7b43.aa7f Vendor1    C4/0/U5        2  No   DF8FE30203010001A326302430120603
BBBB.7b43.aa7f Vendor2    C4/0/U5        2  No   300E0603551D0F0101FF040403020106
AAAA.7b43.aa7f Vendor1    C4/0/U5        2  Yes  820101002D1A264CE212A1BB6C1728B3
DDDD.7b43.aa7f Vendor4    C4/0/U5        2  Yes  7935B694DCA90BC624AC92A519C214B9
AAAA.7b43.aa7f Vendor1    C4/0/U5        2  No   3AB096D00D56ECD07D9B7AB662451CFF

Router#
```

Displaying the Current Dynamic Secrets

In Cisco IOS Release 12.2(15)BC1, the **verbose** option for the **show cable modem** command displays the dynamically generated shared secret (a 16-byte hexadecimal value) that was used in the cable modem's previous registration cycle. The display also shows if the cable modem failed the dynamic shared-secret check or did not download the DOCSIS configuration file from the TFTP server. If a cable modem is offline, its dynamic secret is shown as all zeros.

For example, the following example shows a typical display for a single cable modem that failed the dynamic shared-secret check:

```
Router# show cable modem 00c0.73ee.bbaa verbose

MAC Address                     : 00c0.73ee.bbaa
IP Address                      : 3.18.1.6
Prim Sid                        : 2
QoS Profile Index               : 6
Interface                       : C3/0/U0
```

```
Upstream Power                  : 0.00 dBmV (SNR = 26.92 dBmV)
Downstream Power                : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                   :  2812
Initial Timing Offset           : 2812
Received Power                  :  0.00
MAC Version                     : DOC1.0
Provisioned Mode                : DOC1.0
Capabilities                    : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit                  : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support      : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support      : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs               : 0(Max CPE IPs = 1)
CFG Max-CPE                     : 1
Flaps                           : 26(Feb 14 02:35:39)
Errors                          : 0 CRCs, 0 HCSes
Stn Mtn Failures                : 6 aborts, 0 exhausted
Total US Flows                  : 1(1 active)
Total DS Flows                  : 1(1 active)
Total US Data                   : 0 packets, 0 bytes
Total US Throughput             : 0 bits/sec, 0 packets/sec
Total DS Data                   : 0 packets, 0 bytes
Total DS Throughput             : 0 bits/sec, 0 packets/sec
Active Classifiers              : 0 (Max = NO LIMIT)
Dynamic Secret                  : A3D1028F36EBD54FDCC2F74719664D3F

Router#
```

The following example shows a typical display for a single cable modem that is currently offline (the Dynamic Secret field shows all zeros):

```
Router# show cable modem 00C0.6914.8601 verbose

MAC Address                     : 00C0.6914.8601
IP Address                      : 10.212.192.119
Prim Sid                        : 6231
QoS Profile Index               : 2
Interface                       : C5/1/0/U3
Upstream Power                  : 0.00 dBmV (SNR = 30.19 dBmV)
Downstream Power                : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                   : 1831
Initial Timing Offset           : 1831
Received Power                  : !-2.25
MAC Version                     : DOC1.0
Provisioned Mode                : DOC1.0
Capabilities                    : {Frag=N, Concat=Y, PHS=N, Priv=BPI}
Sid/Said Limit                  : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support      : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support      : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs               : 4(Max CPE IPs = 4)
CFG Max-CPE                     : 4
Flaps                           : 20638(Feb 10 16:04:10)
Errors                          : 0 CRCs, 0 HCSes
Stn Mtn Failures                : 108 aborts, 161 exhausted
Total US Flows                  : 1(1 active)
Total DS Flows                  : 1(1 active)
Total US Data                   : 236222 packets, 146630868 bytes
Total US Throughput             : 0 bits/sec, 0 packets/sec
Total DS Data                   : 9 packets, 1114 bytes
Total DS Throughput             : 0 bits/sec, 0 packets/sec
Active Classifiers              : 0 (Max = NO LIMIT)
Dynamic Secret                  : 00000000000000000000000000000000

Router#
```

Note The Dynamic Secret field shown above is all zeros ("00000000000000000000000000000000"), which indicates that this cable modem is offline.

You can also use the following command to display all the dynamically generated shared secrets that are in use:

```
Router# show cable modem verbose | include Dynamic Secret

Dynamic Secret                      : 434330364346443446433038413132 37
Dynamic Secret                      : 308203E0308202C8A003020102021058
Dynamic Secret                      : 0D06092A864886F70D01010505003081
Dynamic Secret                      : 3037060355040A133044617461204F76
Dynamic Secret                      : 20496E7465726661636520537065636 9
Dynamic Secret                      : 00000000000000000000000000000000
Dynamic Secret                      : 040B130C4361626C65204D6F64656D73
Dynamic Secret                      : 53204361626C65204D6F64656D20526F
Dynamic Secret                      : 7574686F72697479301E170D30313032
Dynamic Secret                      : 313233353935395A308197310B300906
Dynamic Secret                      : 0A133044617461204F76657220436162
Dynamic Secret                      : 6661636520537065636 9666963617469
Dynamic Secret                      : 626C65204D6F64656D73313630340603
Dynamic Secret                      : 65204D6F64656D20526F6F7420436572
Dynamic Secret                      : 747930820122300D06092A864886F70D
Dynamic Secret                      : 010100C0EF369D7BDAB0A938E6ED29C3
Dynamic Secret                      : DA398BF619A11B3C0F64912D133CFFB6
Dynamic Secret                      : FFAD6CE01590ABF5A1A0F50AC05221F2
Dynamic Secret                      : 73504BCA8278D41CAD50D9849B56552D
Dynamic Secret                      : 05F4655F2981E031EB76C90F9B3100D1
Dynamic Secret                      : F4CB0BF4A13EA9512FDE4A2A219C27E9
Dynamic Secret                      : D47BCBB5494E9936D51CB0EB66EF0B0A
Dynamic Secret                      : 8EB196423170B26684BF6730C099D271
Dynamic Secret                      : DF8FE30203010001A326302430120603
Dynamic Secret                      : 300E0603551D0F0101FF040403020106
Dynamic Secret                      : 820101002D1A264CE212A1BB6C1728B3
Dynamic Secret                      : 7935B694DCA90BC624AC92A519C214B9
Dynamic Secret                      : 3AB096D00D56ECD07D9B7AB662451CFF
Dynamic Secret                      : 92E68CFD8783D58557E3994F23A8140F
Dynamic Secret                      : 225A3B01DB67AF0C3637A765E1E7C329
Dynamic Secret                      : 2BB1E6221B6D5596F3D6F506804C995E
Dynamic Secret                      : 45494DC933F8F47A398F69EE6361B017

Router#
```

Troubleshooting Cable Modems with Dynamic Shared Secret

If a cable modem is being marked as having violated the dynamic shared secret, you can enable the following debugs to get more information about the sequence of events that is occurring:

- **debug cable mac-address** *cm-mac-addr* **verbose**—Enables detailed debugging for the cable modem with the specific MAC address.
- **debug cable tlv**—Displays the contents of Type/Length/Value messages that are sent during the registration process.
- **debug cable dynamic-secret**—Displays debugging messages about dynamic shared secret operation.
- **debug tftp server events**—Displays debugging messages for the major events that occur with the Cisco CMTS router's onboard TFTP server.

- **debug tftp server packets**—Displays a packet dump for the DOCSIS configuration files that the TFTP server downloads to a cable modem.

Tip For more information about these debug commands, see the *Cisco CMTS Debugging Commands* chapter in the Cisco Broadband Cable Command Reference Guide, at the following URL:

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_21_debug.html

In addition, examine the messages in the router's log buffer for any helpful information. Use the **show logging** command to display the contents of the router's logging buffer to display these messages. You can limit the output to a specific hour and minute by using the **begin** output modifier. For example, to display only those messages that were recorded at 12:10, give the following command:

```
Router# show logging | begin 12:10
```

Note The exact format for the **begin** output modifier depends on the timestamp you are using for your logging buffer.

Configuration Examples for Dynamic Shared Secret

This section lists a typical configuration for the Dynamic Shared Secret feature.

- Mark Configuration Example, page 24
- Lock Configuration Example, page 25
- Reject Configuration Example, page 25
- Disabled Configuration Example, page 26

Note These configurations also show a shared secret and secondary secret being configured on the cable interface. This is optional but highly recommended, because it adds an additional layer of security during the registration of cable modems.

Mark Configuration Example

The following excerpt from a configuration for the cable interface on a Cisco uBR10012 router configures the cable interface so that cable modems that fail the CMTS MIC check are allowed to come online, but are marked with an exclamation point (!) in the **show cable modem** displays, so that the situation can be investigated further.

```
interface cable c5/1/0
 cable dynamic-secret mark
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Lock Configuration Example

The following excerpt from a configuration for the cable interface on a Cisco uBR7200 series router configures the cable interface so that cable modems that fail the CMTS MIC check are allowed to come online, but are locked into a restrictive QoS configuration that limits the upstream and downstream service flows to a maximum rate of 10 kbps. A locked cable modem remains locked into the restrictive QoS configuration until the modem has remained offline for more than 24 hours, or until you have manually cleared it using the **clear cable modem lock** command.

```
cable qos permission create
cable qos permission update

...

interface cable c3/0
 cable dynamic-secret lock
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Note If you use the **lock** option without specifying a specific QoS profile, you must allow cable modems to create and update QoS profiles, using the **cable qos permission** command. If you do not do this and continue to use the **lock** option without specifying a particular QoS profile, locked cable modems will not be allowed to register until the lock clears or expires.

The following example is the same except that it specifies that the locked cable modem should be assigned QoS profile 90. The cable modem remains locked with this QoS profile until the modem has remained offline for more than 24 hours, or until you have manually cleared it using the **clear cable modem lock** command. Because a specific QoS profile is specified, you do not need to use the **cable qos permission** command.

```
interface cable c3/0
 cable dynamic-secret lock 90
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Note When a locked modem is cleared, it is automatically reset so that it reregisters with the CMTS. It is allowed online with the requested QoS parameters if it registers with a valid DOCSIS configuration that passes the Dynamic Shared Secret checks. However, the modem is locked again if it violates the DOCSIS specifications again.

Reject Configuration Example

The following excerpt from a configuration for the cable interface on a Cisco uBR7200 series router configures the cable interface so that cable modems that fail the CMTS MIC check are rejected and not allowed to register. The cable modem must reregister using a DOCSIS configuration file with a CMTS MIC that matches one of the shared secret or secondary secret values. When it does come online, the CMTS also prints a warning message on the console and marks the cable modem in the **show cable modem** command with an exclamation point (!), so that this situation can be investigated.

```
interface cable c3/0
 cable dynamic-secret reject
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
```

```
...
```

Disabled Configuration Example

The following excerpt from a configuration for the cable interface on a Cisco uBR7100 series router disables the Dynamic Shared Secret feature. In this configuration, the CMTS uses the shared secret and secondary shared secret values unchanged when verifying the CMTS MIC value for each DOCSIS configuration file.

```
interface cable c1/0
 no cable dynamic-secret
 cable shared-secret 7 <primary-shared-secret>
 cable shared-secondary secret index 1 7 <secondary-shared-secret>
...
```

Additional References

For additional information related to Dynamic Shared Secret, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco Broadband Cable Command Reference Guide, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.2 configuration guide	Cisco IOS Release 12.2 Configuration Guides References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
Cisco IOS Release 12.2 command reference	Cisco IOS Release 12.2 Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html
Configuring DOCSIS 1.1 on the Cisco CMTS	"Configuring DOCSIS 1.1 on the Cisco CMTS," in the *CMTS Feature Guide,* at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html
Internal DOCSIS Configurator File Generator for the Cisco CMTS	"Internal DOCSIS Configurator File Generator for the Cisco CMTS," in the *CMTS Feature Guide*, at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html
Cisco Network Registrar End User Guides	Cisco Network Registrar user guides, at the following URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/products_user_guide_list.html
Cisco Broadband Access Center DPE CLI Reference, 2.7.1	Cisco Broadband Access Center DPE CLI REference, 2.7.1, at the following URL: http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/2.7.1/command/reference/cli.html

Standards

Standards[1]	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1

1. Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
No new or modified MIB objects are supported by the Dynamic Shared Secret feature. • CISCO-DOCS-EXT-MIB—Includes attributes to configure the Dynamic Shared Secret feature and to generate traps when a cable modem fails the shared-secret security checks.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

RFCs[1]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Command Summary

Table 1 summarizes the new or modified commands that are needed to configure the Dynamic Shared Secret feature:

Table 1 Command Summary

Command	Purpose
`Router(config-if)# cable dynamic-secret {lock [lock-qos] | mark | reject} [nocrypt]`	Enables the Dynamic Shared Secret feature, so that DOCSIS configuration files are verified with a Message Integrity Check (MIC) that has been created with a dynamically generated shared secret.
`Router(config-if)# cable dynamic-secret exclude {modem mac-address | oui oui-id}`	Excludes one or more specific cable modems from being processed by the Dynamic Shared Secret feature. • **modem** *mac-address*—Specifies the hardware (MAC) address of a specific individual cable modem to be excluded from the Dynamic Shared Secret feature. (You cannot specify a multicast MAC address.) • **oui** *oui-id*—Specifies the organization unique identifier (OUI) of a vendor, so that cable modems from this vendor are excluded from the Dynamic Shared Secret feature. The OUI should be specified as three hexadecimal bytes separated by either periods or colons. Repeat this command for each cable modem MAC address or OUI vendor to be excluded.
`Router# clear cable modem {mac-addr | ip-addr | all | oui string} lock`	Resets the lock on one or more CMs, and reinitializes them, so that they can reregister with a valid DOCSIS configuration file.
`Router# debug cable dynamic-secret`	Displays debugging messages for the Dynamic Shared Secret feature.
`Router# show cable modem`	Enhanced in Cisco IOS Release 12.2(15)BC1 to identify cable modems that fail the dynamic secret authentication checks when the **cable dynamic-secret** command is used with the **mark** and **reject** options. The **show cable modem verbose** command displays more detailed information about specific cable modems.
`Router# show cable modem rogue`	Displays a list of cable modems that have been marked, locked, or rejected because they failed the Dynamic Shared Secret authentication checks.
`Router(config)# snmp-server enable traps cable [cm-chover] [cm-onoff] [cm-remote-query] [dmic-lock] [enfrule-violation] [hccp-failover] [hopping] [usage]`	Enables the sending of Simple Network Management Protocol (SNMP) traps for cable-related events, including Dynamic Shared Secret failures.

For complete information about these commands, and about other cable-specific commands, refer to the *Cisco Broadband Cable Command Reference Guide.* All other commands used with this feature are documented in the Cisco IOS Release 12.2T command reference publications.